2FA Explain (المصادقه الثنائيه)

1- check 000000 - 123456
2- check null
3- reuse previous OTP (used one)
4- reuse code of another account (valid)
5- No rate limit on 2FA =>>
6- check if exposed code in response
7- bypass it by reset password link
- enable 2fa
- logout
- reset password => then click on the link
- if you got into directly then vulnerability

8- bypass it by 0-auth google => 2fa
1- login
2- enable 2fa
3- login with google => if you got into directly then (vulnerability)

9- No rate limit on sending 2FA
10- response manipulation => 403 Forbidden => 200 OK
false => true
0 => 1
failed => successful
11- bypass 2fa by the next step
/login/ => /2FA => /account
/login/ => /account
12- enable 2fa without email verification lead to pre-account takeover
13- enabling 2fa does not end another sessions
change password

- 1 - فالكود اللي بينطلب منك بتجرب تحط 000000 او 123456 علي حسب العدد اللي هوه عايزه

- 2 - تجرب تخش من غير رقم خالص اللي هيا ال null
- لو لازم تحط ارقام بتحط اي ارقام و بتوقف الطلب بالبيرب وتشيل اللي انت حطيته وتكتب مكانه null

- 3 - تجرب تستخدم نفس الكود اكتر من مره لو نفع تبقي ثغره

- 4 - بتجرب تاخد كود بتاع اكونت وتدخل بيه فاكونت تاني بس الاتنين بيبقو مفتوحين مع بعض مستنين الكود يعني تبقي فاتح اكونت ف كروم والتاني ف فايرفوكس مثلا وتاخد كود الاكونت الاول تجرب تخش بيه فالاكونت التاني

- 5 - تجرب تخمن اكواد كتير المفروض بيبقي في limit لازم يوقفك بعد عدد معين لو موقفكش تبقي ثغره
  - لو مفيش limit ابعت الطلب لل intruder وخليها يخمن

- 6 - تتاكد ممكن يكون الكود رجع ف ال Response
  - وانت بتسجل بتوقف الطلب قبل ما تضغط log in وتشوف الكود ف ال Response

---

- 7 - لو قدرت تتخطي ال 2FA عن طريق link ال reset password
  - بتعمل reset password وهتغير الباس عن طريق اللينك وتخش علي الاكونت من غير الكود (OTP)

- 8 - لو انت رابط الاكونت بجوجل مثلا ومفعل ال 2FA
  - بتيجي تسجل دخول تاني فالعادي بتسجل بالايميل والباس وبيطلب كود
  - انت تجرب تخش بايكونه جوجل علطول لو مطلبش منك كود علشان 2FA تبقي كدا ثغره

- 9 - الاول كان تخمين دا انك تبعت رسايل كتير وميقاش في limit لو بعت معاك كود 2FA كتير تبقي ثغره

```
ahmed@gmail.com => 123  => Otp 1111 do intercept

successful
                    I



carlos: Montoya  => 0000 => do intercept

fail => successful
```

- 10 - بتغير ف ال response
Forbidden => 200 OK 403
false => true
1 <= 0
failed => successful

- 11 - بتعمل اكونت للـ test وتاخد المسارات بتاعت الصفحات

```
/login
/login2 =>
/my-account?id=wiener
```

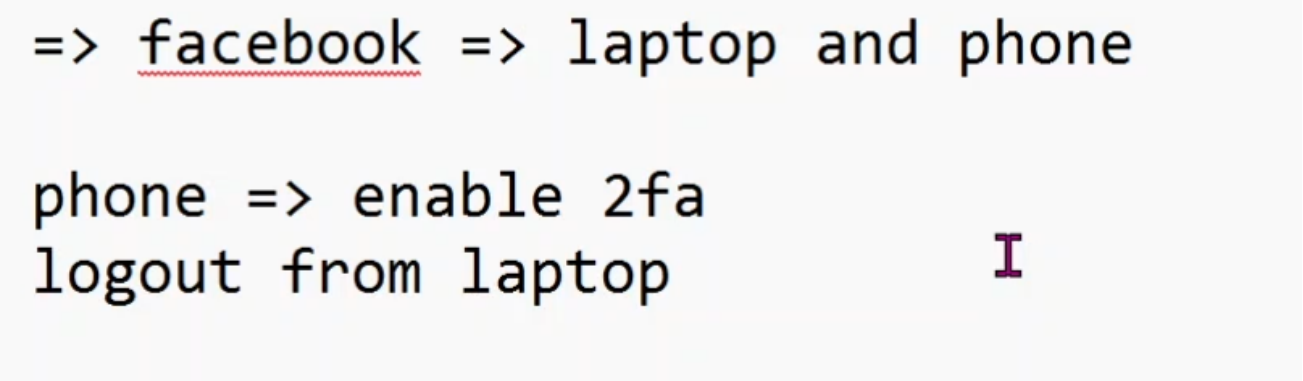
- وتدخل تاني تجرب بس بتيجي تعمل Bypass لصفحه 2FA يعني تحط المسار بتاع الصفحه اللي بعدها وتشوف

- 12 -

```
register => hossam@gmail.com => login => don't confirm
settings => enable 2FA => pre-account takeover
```

- بتعمل اكونت جديد بس مش بت Active الاكونت وتسجل دخول لو قدرت تفعل ال 2FA تبقي ثغره

- 13 -



- لو الاكونت متسجل ف اكتر من جهاز
- لو فعلت ال 2FA من جهاز المفروض يخرج من الباقي لو مخرجش تبقي ثغره